Claims

We claim:

1. A method for authenticating d_i identities using two prime numbers p and q such that $q \mid p - 1$, each identity includes a private key s_i and a public key v_i, and a publicly known generator is α such that $\alpha^q \equiv 1 \ (mod\ p)$, comprising:

providing, a verifier, with an ordered list of the public keys v_i;

selecting uniformly at random, by a prover, a non-negative number r less than q;

sending a number $x = \alpha^r \ (mod\ p)$ from the prover to a verifier;

selecting uniformly at random, by the verifier, a non-negative number e less than $2^{(t+logd)}$, where log is base 2, and a number t is a predetermined security parameter;

receiving by the prover from the verifier the number e;

generating, by the prover, a number $y = r + \Sigma_i s_i * e^i \ (mod\ q)$;

sending by the prover to the verifier the number y;

determining if an equality $x = \alpha^y * \Pi_i (v_i)^{e^i} \ (mod\ p)$ is true; and

accepting the prover as having the d_i identities if and only if the equality is true.

2. The method of claim 1, in which the security parameter is 95.

3. The method of claim 1, in which the sending and receiving by the prover is performed by a single LED of an optical communications device.

4. The method of claim 4, further comprising:

driving the LED in forward bias to emit light; and

driving the LED in reverse bias to sense light.

5. The method of claim 1, in which the LED is coupled to pins of a microcontroller via a current limiting resister, and the microcontroller is operated by a switch.

6. The method of claim 3, in which the LED operates as a flashlight while authenticating.

7. The method of claim 1, in which the sending and receiving by the prover is performed by a microcontroller of a smart card.

8. The method of claim 1, in which the generating uses a fast Fourier transform.

9. The method of claim 1, further comprising:

storing, in a memory accessible by the prover, a table, for each private key v_i, a residue modulo q of a product of the private key v_i with numbers n expressed as powers of 2 from 2^1 to $2^{1+\log q}$; and

multiplying a particular private key with a particular number n by adding the corresponding residue to the private key.

10. The method of claim 1, further comprising:

storing in a memory accessible by the prover, for each residue modulo q of a product of e with powers of 2 from 2^1 to $2^{1+\log q}$.